CLAIMS

What is claimed is:

1. A method for use in curve-based cryptographic logic, the method comprising:

determining at least one curve for use in cryptographically processing selected information; and

determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve.

2. The method as recited in Claim 1, wherein said at least one curve includes an elliptic curve.

3. The method as recited in Claim 1, wherein said pairings include Weil pairings.

4. The method as recited in Claim 1, wherein said pairings include Squared Weil pairings.

5. The method as recited in Claim 1, wherein said pairings include Tate pairings.

6. The method as recited in Claim 1, wherein said pairings include Squared Tate pairings.

7. The method as recited in Claim 1, further comprising:

cryptographically processing said selected information based on said pairings.

8. The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

9. The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

10. The method as recited in Claim 7, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

11. The method as recited in Claim 2, wherein determining said pairings for use in cryptographically processing said selected information further includes:

determining at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve;

determining said parabola that is associated with said multiples of a point, and a line associated with said parabola;

determining a third function based on said parabola and said line; and

determining said pairings based on said third function.

12. The method as recited in Claim 11, wherein:

said elliptic curve includes an elliptic curve E over a field K;

said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;

said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;

said line is a vertical line through

$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$

said third function includes $f_{2j+k,\,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X})-x_4\right)}.$$

13. The method as recited in Claim 12, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

14. The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

parab $(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1\ \lambda_2)$

$+ (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$; and

said third function includes $f_{2j+k,\ \boldsymbol{P}}\ (\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X})\, f_{k,\boldsymbol{P}}(\boldsymbol{X})\, f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

15. The method as recited in Claim 14, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

16. The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

parab$(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_2)(x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1\ \lambda_2)$

$+ (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\boldsymbol{X}))$

said third function includes $f_{2j+k,\ \boldsymbol{P}}\ (\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X})\, f_{k,\boldsymbol{P}}(\boldsymbol{X})\, f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

17. The method as recited in Claim 16, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

18. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining at least one curve for use in cryptographically processing selected information;

calculating pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve; and

cryptographically processing said selected information based on said pairings.

19. The computer-readable medium as recited in Claim 18, wherein said at least one curve includes an elliptic curve.

20. The computer-readable medium as recited in Claim 18, wherein said pairings include at least one type of pairings selected from a group of different pairings comprising Weil pairings, Squared Weil pairings, Tate pairings, and Squared Tate pairings.

21. The computer-readable medium as recited in Claim 18, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

22. The computer-readable medium as recited in Claim 18, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

23. The computer-readable medium as recited in Claim 21, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

24. The computer-readable medium as recited in Claim 19, wherein calculating said pairings further includes:

calculating at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve;

calculating said parabola that is associated with said multiples of a point, and a line associated with said parabola;

calculating a third function based on said parabola and said line; and

calculating said pairings based on said third function.

25. The computer-readable medium as recited in Claim 24, wherein:

said elliptic curve includes an elliptic curve E over a field K;

said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;

said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;

said line is a vertical line through

$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$

said third function includes $f_{2j+k,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X})-x_4)}.$$

26. The computer-readable medium as recited in Claim 25, further including:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

27. The computer-readable medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X})-x_1)(x(\boldsymbol{X})+x_1+x_3+a_2+\lambda_1\lambda_2) + (\lambda_1+\lambda_2+a_1)(y_1-y(\boldsymbol{X}));$$ and

said third function includes $f_{2j+k,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X})-x_4)}.$$

28. The computer-readable medium as recited in Claim 27, further including:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

29. The computer-readable medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_2)(x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) \\ + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\boldsymbol{X}))$$

said third function includes $f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

30. The computer-readable medium as recited in Claim 29, further including:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

31. An apparatus comprising:

memory configurable to store information; and

logic operatively coupled to said memory and configurable to at least support cryptographic processing of selected information stored in said memory by determining at least one curve for use in cryptographically processing selected information and determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve.

32. The apparatus as recited in Claim 31, wherein said at least one curve includes an elliptic curve.

33. The apparatus as recited in Claim 31, wherein said logic is further configurable to perform said cryptographic processing of said selected information.

34. The apparatus as recited in Claim 31, wherein said pairings include at least one type of pairings selected from a group of different pairings comprising Weil pairings, Squared Weil pairings, Tate pairings, and Squared Tate pairings.

35. The apparatus as recited in Claim 31, wherein said cryptographic processing of said selected information includes decrypting said selected information and outputting corresponding decrypted information.

36. The apparatus as recited in Claim 31, wherein said cryptographic processing of said selected information includes encrypting said selected information and outputting corresponding encrypted information.

37. The apparatus as recited in Claim 35, wherein said cryptographic processing at least supports at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

38. The apparatus as recited in Claim 32, wherein said logic is further configured to calculate at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve, calculate said parabola that is associated with said multiples of a point, and a line associated with said parabola, calculate a third function based on said parabola and said line, and calculate said pairings based on said third function.

39. The apparatus as recited in Claim 38, wherein:

said elliptic curve includes an elliptic curve E over a field K;

said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;

said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;

said line is a vertical line through

$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$

said third function includes $f_{2j+k,\ \boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X})-x_4)}.$$

40. The apparatus as recited in Claim 39, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

41. The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

parab $(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1\ \lambda_2)$
$+ (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$; and

said third function includes $f_{2j+k,\ \boldsymbol{P}}\ (\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X})-x_4)}.$$

42. The apparatus as recited in Claim 41, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

43. The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

$$\begin{aligned}\text{parab}(\boldsymbol{X}) &:= (x(\boldsymbol{X}) - x_2)(x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) \\ &\quad + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\boldsymbol{X}))\end{aligned}$$

said third function includes $f_{2j+k,\, \boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

44. The apparatus as recited in Claim 43, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.